OS Command Injection on Chamilo LMS

High **ywarnier** published **GHSA-crc6-r6c7-44q3** 9 hours ago

Package

Chamilo LMS (PHP)

Affected versions

2.0.0-rc

Patched versions

2.0

Description

Vulnerability Report: OS Command Injection on Chamilo LMS

1. Vulnerability Overview

Product: Chamilo LMS
Version: <2.0 (Confirmed)
Vulnerability Type: OS Command Injection (CWE-78)
Impact: Authenticated Remote Code Execution (RCE)
Severity: High
Auth Required: Yes (Authenticated User with poisoned session)

2. Description

A critical OS Command Injection vulnerability exists in the `main/inc/ajax/gradebook.ajax.php` endpoint of Chamilo LMS v1.11.32. The `export_all_certificates` action handles the export of course certificates by executing a background PHP script via `shell_exec`.

The application retrieves the course code using `api_get_course_id()`, which derives its value from the `$_SESSION['_cid']` session variable. This value is subsequently concatenated directly into a shell command string without any sanitization or escaping (e.g., using `escapeshellarg()`). If an attacker can manipulate or poison their session data to inject arbitrary shell metacharacters into the `$_SESSION['_cid']` variable, they can achieve arbitrary command execution on the underlying server.

3. Technical Details

- **Vulnerable File:** `/main/inc/ajax/gradebook.ajax.php`
- **Vulnerable Function:** `export_all_certificates` case.
- **Root Cause Analysis:**

When a user triggers the `export_all_certificates` action, the script attempts to run a background process for processing certificates:

```
$courseCode = api_get_course_id(); // Retrieves the value from $_SESSION['_cid']
$sessionId = api_get_session_id();
// ...
$commandScript = api_get_path(SYS_CODE_PATH).'gradebook/cli/export_all_certificates.php'
$userList = implode(',', $userList);

// Flaw: Variables like $courseCode are passed directly to the shell without escapeshell
shell_exec("php $commandScript $courseCode $sessionId $categoryId $userList > /dev/null
```

Because the application implicitly trusts the contents of the session variables and fails to properly escape them before sending them to the system shell, an attacker with a manipulated session can append and execute malicious commands. For example, if `_cid` contains `"; touch /tmp/remote_code_by_k; #"`, the command interpreted by the bash/sh shell becomes:

```
php /path/to/script.php ; touch /tmp/remote_code_by_k; # ... > /dev/null &
```

The shell executes the CLI script, followed by the injected payload, and ignores the rest of the intended command string.

4. Proof of Concept Strategy

(confidential)

5. Impact Analysis

- **Confidentiality:** Attacker gets full access to read system files, application source code, and configuration files containing database credentials.
- **Integrity:** Attacker can alter, deface, or sabotage the application, database, and filesystem.

- **Availability:** Attacker can bring down the server by deleting files, exhausting resources, or installing ransomware.
- **CVSS v3.1:** 8.8 (High) - `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`

6. Recommendations & Remediation

- **Apply `escapeshellarg()`:** Wrap all user-derived variables (like `$courseCode`, `$sessionId`, and `$userList`) with PHP's `escapeshellarg()` before passing them to `shell_exec()` to neutralize arbitrary OS metacharacters.
- **Strict Session Validation:** Ensure variables stored in the session state (e.g., `$_SESSION['_cid']`) are rigidly typed and sanitized so that potential "Session Poisoning" or IDOR chaining attacks are blocked at the entry point.
- **Enforce Least Privilege:** Configure the web server service (`www-data`) with restrictive filesystem write permissions and limit application access to essential Linux shell binaries to mitigate post-exploitation capabilities.

7. Fix

`62671e5`
or update to Chamilo v2.0 stable

Severity

High 8.8 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE ID

CVE-2026-35196

Weaknesses

▶ CWE-78

Credits

kx00007 Reporter